

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA

v.

22-CR-6009-CJS-MJP

JOHN DOUGLAS LOONEY,

Defendant.

GOVERNMENT’S RESPONSE TO DEFENDANT’S MOTIONS

The United States of America, by and through its attorneys, Trini E. Ross, United States Attorney for the Western District of New York, and Meghan K. McGuire, Assistant United States Attorney, hereby responds to defendant’s motions (Dkt. 62).

FACTUAL BACKGROUND

On April 5, 1994, the defendant plead guilty to a one-count superseding indictment that charged him with possession of child pornography. The defendant was sentenced to 90 days imprisonment, 90 days of home confinement, 450 hours of community service, and 3 years’ supervised release.

In 2018 and 2019, Federal Bureau of Investigations (FBI) Task Force Officer (Ofc.) Carlton Turner was investigating the illegal exchange of child pornography on a particular peer-to-peer file sharing network (hereinafter the “Network”). On three separate occasions, Ofc. Turner observed requests for child pornography files coming from an IP address that was registered to the defendant’s residence.

Based on these requests and the defendant's prior conviction, Ofc. Turner sought and obtained a warrant from the Hon. Marian W. Payson to search the defendant's residence for evidence of the possession and distribution of child pornography.

In Ofc. Turner's supporting affidavit, he explained how the Network operated as follows:

8. When a user uploads a file into the Network, the software breaks the file into pieces (called "blocks") and encrypts each block.

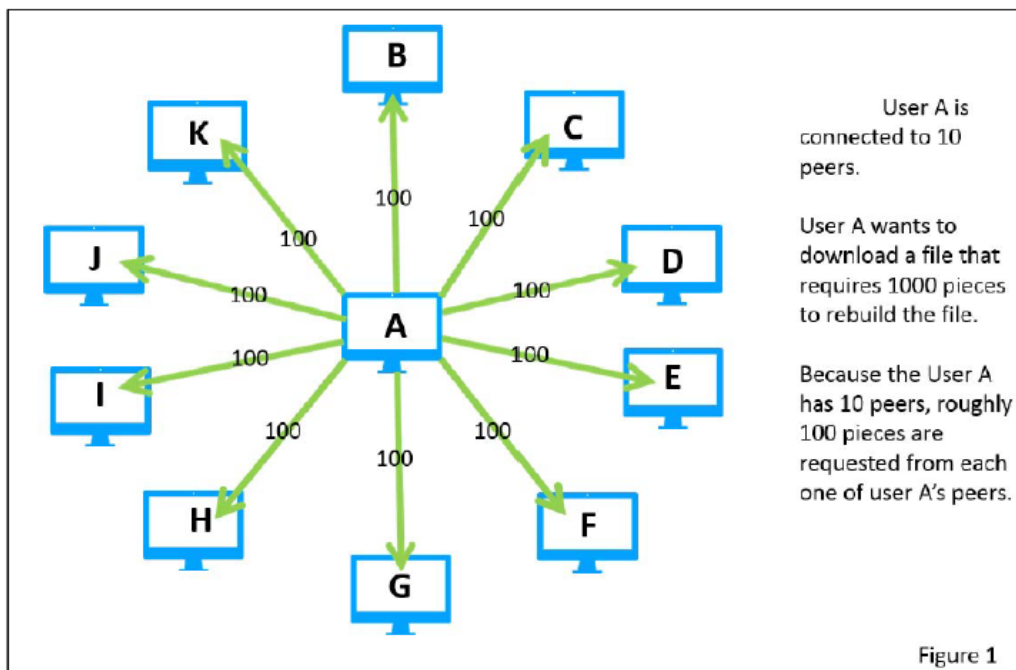
9. The encrypted blocks are then randomly distributed and stored on individual users' computers throughout the Network.

10. In order for a file to be reassembled and downloaded, the software creates an index of all blocks necessary to reconstruct the file.

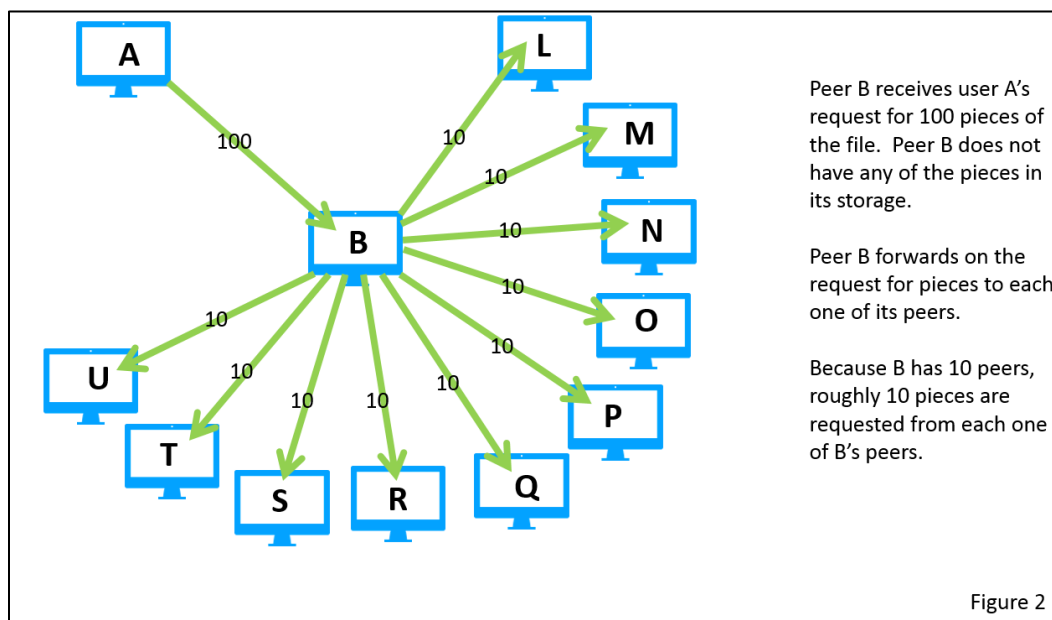
...

15. When a user attempts to download a file, the Network first downloads the piece of the file containing the index, which provides the information required to retrieve the individual pieces of the file (i.e., the blocks). The Network software then requests all of the necessary blocks from the requesting user's peers. Rather than request all of the blocks from a single peer, the Network software divides the requests for blocks into roughly equal amounts among the requesting user's peers. If a user's peer does not have the particular block(s) being requested in its storage, that peer will then divide up the remaining requests and ask its peers for the block(s).

16. For example, if User "A" has 10 peers and requests 1000 blocks of a file, roughly 100 blocks are requested from each one of User A's peers. See Figure 1.



17. If Peer "B" receives User A's request for 100 blocks of the file, but does not have any of those blocks in its storage, Peer B forwards on the requests to Peer B's peers. If Peer B has 10 peers of its own, roughly 10 blocks are requested from each one of Peer B's peers. See Figure 2.



(Turner Aff., Def. Motion, Dkt. 62-1, p. 23-80.)

Ofc. Turner's affidavit explained how law enforcement investigates the trafficking of child pornography on the Network:

31. A modified version of the Network software is available to sworn law enforcement officers to assist in conducting Network investigations. I have been trained on the operation of the modified law enforcement version of the Network.

...

33. The information logged by law enforcement includes, but is not limited to: the IP addresses of the law enforcement computer's peers; the number of peers those peers report to have; a unique identifier assigned by the software (referred to as the computer's Network "location"); the remaining number of times a request for a piece of a file may be forwarded; the date/time of requests received from a peer; and the digital hash value of a requested piece.

(Id.)

Ofc. Turner's affidavit explained how this information was put into a mathematical formula (hereinafter the "Formula") to determine whether a particular device was attempting to download child pornography:

43. Your affiant has reviewed a peer-reviewed, published, and publicly available academic paper that describes the methodology behind this mathematical formula.

44. In basic terms, the formula uses three known variables—(a) the approximate minimum and maximum number of blocks the original requestor could request, in total, from its peers; (b) the number of blocks requested from the law enforcement computer; and (c) the number of peers the requesting computer has—and one assumption—(d) that the original requestor (if it is not the computer directly connected to the law enforcement computer) has 8 peers.¹

¹ The formula assumes that, in a scenario where the law enforcement computer is two degrees of separation from the original requestor, the original requestor has 8 peers. This is a very conservative estimate because the average user has significantly more than 8 peers. As a result, the formula will underestimate the likelihood that a request is received from an original

45. Then, relying on the fact that an original or first-level request is divided in approximately equally parts between each of the original requestor's peers and an intermediary or second-level request is subdivided evenly between the intermediary user's peers (*see* Figures 1 and 2), the formula determines whether it is more probable than not that a request received by a law enforcement computer for a specific number of blocks of a known "file of interest" was received from an original requestor or a mere intermediary.

46. For example, assume File of Interest A requires a minimum of approximately 6,000 blocks to download. An initial request could seek anywhere from approximately 6,000 to 12,000 blocks to download this file.

47. The law enforcement computer receives a request for 100 blocks of File of Interest A from User X. Through the request, law enforcement is also informed that User X has 50 peers and that the request can be forwarded 18 times.

48. If User X were the original requestor, then a recipient of a request from User X would expect to receive a request for somewhere between **120 blocks** (6,000 minimum necessary blocks/50 peers) and **240 blocks** (12,000 maximum necessary blocks/50 peers).

49. If, in the alternative, User X were a second level requestor, then User X likely received a request from the original user for anywhere from 750 blocks (6,000 minimum required blocks/8 peers) to 1,500 blocks (12,000 maximum required blocks/8 peers). A recipient of a second-level request from User X would then expect to receive a request for anywhere from approximately **15 blocks** (750 requested blocks/50 peers) to **30 blocks** (1,500 blocks/50 peers).

50. Note that the number of requests the law enforcement computer receives if User X is an original requestor is substantially larger (often by a factor of 10) than the number of requests the law enforcement computer would receive if User X were merely a second-level or intermediary requestor.

51. In this example, the law enforcement computer received a request for 100 blocks. That request falls much closer to the expected range for an original request from User X (120-240). In contrast, a request for 100 blocks is substantially greater than the expected range for a second level request from User X (15-30 blocks). Therefore, there is a high probability that User X was the original requestor of File of Interest A.

requestor; this conservative assumption will identify fewer actual original requestors than actually exist.

(*Id.*)

Ofc. Turner's affidavit stated that the Formula employed in his investigation was peer reviewed and had been tested for accuracy:

52. The peer reviewed and published academic paper referenced above contains a detailed evaluation of this methodology and concludes that the formula is highly accurate in differentiating original requestors from second-level/intermediary requestors.

53. Specifically, the authors of this paper tested the formula using over 26,000 test runs. In those test runs, the formula has an approximately 2% false positive rate (i.e., it misidentified an intermediary requestor as an original requestor only 2% of the time).

54. Based upon my training and experience, I believe this to be a reliable method to determine whether it is significantly more probable than not that that a given computer using the Network is the original requestor of a file of interest.

(*Id.*)

Ofc. Turner expressed his belief that the Formula was a reliable method of establishing probable cause. But he also disclosed to the Court that it was not perfect: in application, it had a false positive rate of approximately 2%.

In addition to relying upon the fact that the Formula was peer-reviewed and tested, Ofc. Turner's affidavit noted that he had training and experience that reinforced his belief that the Formula was reliable:

55. I am also aware through my training and experience that dozens of searches of digital devices have been conducted by law enforcement officers (either through court-authorization or consent) related to targets whose IP addresses were identified based upon analysis of information from the Network's law enforcement computers, pursuant to which evidence of child pornography possession was located.

(*Id.*)

Moreover, Ofc. Turner's affidavit relied upon and attached a thoroughly-reasons decision upholding the use of the Formula as a basis for determining probable cause:

56. Further, search warrants issued on the basis of the above-described formula have consistently withstood judicial scrutiny on a motion to suppress. As an example, enclosed herewith as **Attachment C** is a decision from Magistrate Judge Nannette A. Baker, Easter District of Missouri, in the case entitled denying a defendant's motion to suppress a search warrant obtain on the basis of this formula.

(*Id.*)

On March 1, 2019, the FBI executed the warrant at the defendant's residence. Prior to executing the search warrant, Ofc. Turner and FBI Special Agent (SA) Barry Couch interviewed the defendant. During this interview, the defendant admitted that he used the Network to download files of child pornography.

While executing the search warrant, the FBI found three laptops in the defendant's residence. In total, these laptops contained over 1 million images and videos of child pornography.

The FBI also found a pair of thumb drives that contained a folder named after the Network. The Network folder contained approximately 300 manifest keys² for child pornography files.

² Unlike other file sharing systems, the Network does not have a search function whereby users can search certain terms to locate files. Instead, the Network's software creates a unique key – a series of letters, numbers, and special characters – that is used to download any given file. Some of the keys contain words or phrases that describe the contents of the file. To

On January 18, 2022, a federal grand jury returned a three-count Indictment against the defendant, charging him with possessing child pornography, in violation of Title 18, United States Code, Section 2252A(a)(5)(B) and (b)(2). (Dkt. 36.)

On February 4, 2022, the government filed its Notice of Intent to Use Evidence (Dkt. 41) advising the defendant of its intent to offer the items seized during the execution of the search warrant—including the three laptops that contained over 1,000,000 child pornography files and the two thumb drives that contained child pornography manifest keys—as evidence at trial.

DISCUSSION

A. THE DEFENDANT’S MOTION TO SUPPRESS SHOULD BE DENIED

a. The Warrant to Search the Defendant’s Residence was Supported by Probable Cause

“The Fourth Amendment . . . prohibits the issuance of warrants without ‘probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.’” *United States v. Jones*, 43 F.4th 94, 108 (2d Cir. 2022) (quoting U.S. Const. Amend. IV).

download a file on the network, a user must have the key for the file. A user who wishes to locate and download a file can obtain the key from: (a) a message board within the Network; (b) a website within the Network; or (c) another Network user. Once a user obtains the key associated with the file that he or she wants to download, the user must enter that exact key into the “download” box on the network’s “file sharing” page.

“The Amendment's text makes clear that the ultimate touchstone of the Fourth Amendment is ‘reasonableness.’ When the police undertake a search to discover evidence of criminal wrongdoing, reasonableness generally requires the obtaining of a judicial warrant. Warrants ensure that the inferences to support a search are drawn by a neutral and detached magistrate instead of being judged by the officer engaged in the often competitive enterprise of ferreting out crime. Because warrants must be supported by probable cause, warrants not so supported are invalid.” *Id.* (quotations omitted).

“Probable cause is not a high bar. To determine whether probable cause to search exists, an issuing magistrate must make a practical, common-sense decision whether, given all the circumstances set forth in an affidavit, there is a fair probability that contraband or evidence of a crime will be found in a particular place.” *Id.* at 109.

“Because probable cause deals with probabilities and depends on the totality of the circumstances, it is a fluid concept that is not readily, or even usefully, reduced to a neat set of legal rules. Probable cause is a practical, common-sensical, and all-things-considered standard. It requires only the kind of fair probability on which reasonable and prudent people, not legal technicians, act.” *Id.*

“When reviewing the validity of a search warrant the duty of the court is simply to ensure that the magistrate had a substantial basis for concluding that probable cause existed.” *United States v. Forbes*, No. 20-CR-6140-FPG-MJP, 2022 WL 6786271, at *13 (W.D.N.Y. June 10, 2022), *report and recommendation adopted*, No. 20-CR-06140-FPG, 2022 WL 4545256 (W.D.N.Y. Sept. 29, 2022) (quotations omitted). “A search warrant issued by a neutral and

detached magistrate is entitled to substantial deference, and doubts should be resolved in favor of upholding the warrant.” *Id.* (quotations omitted).

“After-the-fact scrutiny by courts of the sufficiency of an affidavit applying for a warrant should not take the form of de novo review.” *Id.* (quotation omitted). “Resolution of doubtful or marginal cases in this area should be largely determined by the preference to be accorded to warrants.” *Id.* (quotation omitted).

Here, Ofc. Turner’s affidavit provided ample, detailed information to support Judge Payson’s finding of probable cause. Ofc. Turner explained the logic underpinning the Formula. He qualified that it was based on a model that “roughly” approximated the Network’s operation. He disclosed the assumptions that were made in creating the Formula. He said that the Formula had been tested and it was not perfect but had a false positive rate of only approximately 2%. He revealed that the Formula had been employed by law enforcement to obtain warrants in the past and, to his knowledge, had never been wrong.

Ofc. Turner then turned to the investigation at hand and explained what information that he collected while operating on an undercover capacity on the Network, how he applied that information to the Formula, and what conclusions he reached. On top of this, Ofc. Turner added the fact that the defendant had a prior conviction for possessing child pornography.

The defendant alleges, in general, that the warrant lacked probable cause because it “relies upon a false formula.” (Def. Motion, Dkt. 62, p. 7.) The defendant alleges the Formula is “false” because it assumes that: (a) requests for blocks are distributed roughly

evenly among a user's peers³, (b) an intermediary peer has 8 peers, and (c) all peers are continuously communicating⁴.

But the logic of these assumptions is irrelevant to this Court's analysis. The relevant question is does the Formula accurately predict whether a computer is likely to be requesting a download (as opposed to merely relaying a request for a download). The question is whether the Formula works in most instances. And it does.

Dog sniffs are a good analogy. Does a warrant application typically include the science behind why and how a dog's nose is able to detect contraband? No. But the

³ The defendant insists that the Network was designed to distribute requests unevenly by sending a greater number of requests to certain peers based on a number of specific characteristics. The government does not concede the accuracy of this description and the defendant has offered no admissible proof to support it.

In fact, Dr. Levin explained in the *Dickerman* hearing that, while that defendant's description of the Network's operation may be what its developers intended, it is not how the Network actually operates. Dr. Levin and others have studied the actual operation of the Network and concluded that requests (Dkt. 62-5, p. 185-86 ("So there's -- there's this idea of what Freenet is trying to do and then there's what Freenet actually does. And in reality people, not me but other published papers, have actually looked at the topology of Freenet and decided whether it was -- what type of -- you know, whether it was this topology or that topology. So in the end, although it attempts to have a particular nice topology with certain mathematical properties, it edges towards this sort of lazy one. And so we evaluated both as has been done in previous papers. And by running both, we determined that -- that this -- you know, exactly what I said; that modeling things as a uniform distribution is a -- or a uniform distribution is a nice model to distinguish between the relayer and the requester."))

However, for the purposes of this motion, it is irrelevant whether the even-share distribution model is a perfect or imperfect model of how Freenet actually operates because any imperfections in the model do not, in practice, undermine the reliability of the Formula in predicting whether a user is more likely than not the original requestor of a particular file.

⁴ It is not clear that the Formula requires this assumption. Ofc. Turner's Affidavit explains that "[i]t is typical for a user's number of peers to change from minute to minute. Thus, the formula uses the average number of peers a user has throughout the duration of a given download attempt." (Turner Aff., Dkt. 62-1, n. 7.) As such, intermittent disconnections are accounted for.

application does represent that a trained narcotics dog accurately alerts in the presence of narcotics more often than it inaccurately alerts. How does the officer signing the affidavit know that? Because the theory has been tested and employed in real-world situations. Most times—not every time, but most times—the dog’s alerts are accurate. There are plenty of variables that, in real world operation, can lead a dog to alert inaccurately. And that happens sometimes. But, in the aggregate, the dog alerts correctly. That is sufficient to establish probable cause.

The same is true here. Yes, the Formula is based on some assumptions and modeling. Sometimes that will lead to inaccurate results. Sometimes, that will result in the false positives depicted in the Defendant’s motion at pages 26, 28, and 30.

That is precisely why the Formula was tested on Freenet before it was employed by law enforcement and the false positive rate was disclosed. As Dr. Brian Levin explained in the *Dickerman* case:

So in order to evaluate the false positive read of our algorithm, we actually got on the network and took traces of -- of -- I’m sorry. We got on the network and we looked at the messages that were directed to us; that were sent to us by our Freenet peers that we were supposed to look at, and we looked at ones that we knew were not requesters.

Now I haven't quite explained this, but we had talked a bit about the “Hops To Live” field, and let me just say this little detail. A Hops To Live of 16 definitely means you’re not looking at the requester. So we can take messages that were directed to us that have Hops To Live of 16. We know that these are not requests for the file. They're not sent by someone who’s requested the file, and then we can run those messages against our algorithm. And so when we did that, we found that the false positive read was two percent, roughly.

So in sum . . . we looked at the false positive read by actually applying it to Freenet data. And what's nice about that is it has ground truth; right?

And so -- so we're -- we're quite confident in those results. And those results are published now and peer reviewed, and the methodology we used was completely accepted by the -- by the reviewers.

(Dkt. 62-5, p. 165-66.)

For example, when asked about the impact of the continuous connectivity assumption on the accuracy of the Formula, Dr. Levine explained that that was precisely what the false positive metric accounted for:

[W]hat the false positive rate test we did includes is those types -- I mean this was 26,000 different runs over a period of months as described in the paper. And during some of those months, some of these things you're speculating about happened or didn't. To the extent that they happened, they were captured by the test. So any speculation is -- about what may or may not occur is just speculation; whereas, the false positive rate test was on real data with real events that happened, such as bad connections.

...

Now are those a problem for the test? In my experience, it's a problem 2.3 percent of the time in my estimation.

(Dkt. 62-5, p. 189-90.)

The Formula has been tested. About 2% of the time, the assumptions underlying the Formula—which, according to the defendant, include assumptions about even share distribution, 8 peers per intermediary, and continuous operation of all peers—lead to an inaccurate result. The rest of the time, the Formula accurately predicts whether a computer is requesting a download (as opposed to merely relaying a request for a download). *See United States v. Weyerman*, 19-CR-0088-PD (E.D. Pa. Jan. 3, 2020), *aff'd*, 2022 WL 1552997 (3d Cir. May 17, 2022) (“A product of significant research and a deep knowledge of Freenet, the Algorithm is extraordinarily reliable, showing 98 to 100% accuracy in distinguishing between

original requesters and relayers of Network files.”). That is sufficient to establish probable cause.

The defense has offered zero evidence to undermine the accuracy of the Formula’s prediction. It has not presented evidence of a single study of the Formula that resulted in a substantially higher false positive rate.⁵ It has not presented evidence of a single case in which the Formula was used to obtain a search warrant and no child pornography was found. Thus, the defense’s motion has done nothing to undermine the reliability of the Formula.

The defendant’s motion attaches a pair of “articles” from an undisclosed source with unnamed authors going by the pseudonym “Freenet Project Inc.” (Dkt. 62-6 and 62-8.) The “articles,” like the defendant’s motion, challenge certain assumptions that underlie the Formula. They also speculate that, in theory, the Formula should not work because of the underlying assumptions. But they say nothing about the reliability of the Formula in practice.

The remaining articles cited by the defendant discuss the operation of Freenet. But, once again, none of the articles say anything about whether the Formula works and reliably predicts whether a user is a downloader.

Even if the defendant’s supporting articles contained information that undermined the reliability of the Formula (which they do not), the defendant has not established that any of these articles can properly be considered by the Court during an evidentiary hearing. The defendant has not alleged that any of these articles were published in peer reviewed

⁵Technically, any false positive rate less than 50% should still be sufficient to support a finding of probable cause because it is still more likely than not (*i.e.*, probable) to be an accurate indicator of the source of a download request.

publications. The defendant has not submitted an affidavit from the authors of any of these articles or a qualified expert.⁶ The defendant has not even suggested that the authors or a qualified expert might testify at an evidentiary hearing.

The defendant has submitted nothing more than a collection of documents printed from the internet that theorize the Formula should not work. But you can find support for any theory on the internet. For example, if you google “birds are not real,” you’ll find millions of webpages that assert birds are actually drones operated by the government to spy on American citizens, along with “evidence” and “logical” arguments demonstrating why the theory must be true. Many, like the documents submitted by the defendant, are written by unnamed groups operating under a pseudonym. Certainly, if I printed some of these pages and attached them to a motion, I would not be entitled to an evidentiary hearing on whether birds are in fact real. The point is that, in a court of law, it is not enough to find something on the internet that supports your argument. The defendant had to submit evidence that raised a substantial issue of fact regarding the validity of the warrant. He failed to do so.

In the end, Ofc. Turner’s affidavit gave Judge Payson a substantial basis to assess the reliability of the Formula and determine that, coupled with the evidence of the defendant’s prior conviction for possession of child pornography, there was probable cause to believe evidence of child pornography crimes would be in the defendant’s residence. As such, the defendant’s motion to suppress should be denied.

⁶ In *Dickerman*, in contrast, the defendant submitted an affidavit from his proposed expert before he was entitled to a hearing. (See *Dickerman* Decision, Dkt. 62-1, p. 10.)

b. The Warrant was not Stale

A court “may conclude that a warrant lacks probable cause where the evidence supporting it is not sufficiently close in time to the issuance of the warrant that probable cause can be said to exist as of the time of the search—that is, where the facts supporting criminal activity have grown stale by the time that the warrant issues.” *United States v. Wilbert*, 818 F. App’x 113, 114 (2d Cir.), *cert. denied*, 141 S. Ct. 639 (2020) (quotation omitted). “The two critical factors in determining whether facts supporting a search warrant are stale are the age of those facts and the nature of the conduct alleged to have violated the law.” *Id.* (quotation and citation omitted).

“The determination of staleness in investigations involving child pornography is unique.” *United States v. Raymonda*, 780 F.3d 105, 114 (2d Cir. 2015) (quotation omitted). “Because it is well known that images of child pornography are likely to be hoarded by persons interested in those materials in the privacy of their homes, evidence that such persons possessed child pornography in the past supports a reasonable inference that they retain those images—or have obtained new ones—in the present.” *Id.* (quotations and citations omitted). “[T]he value of that inference in any given case depends on the preliminary finding that the suspect is a person interested in images of child pornography.” *Id.*

In this case, less than six months passed between the date when Ofc. Turner received his third download request from the defendant’s computer (September 11, 2018) and the dates when Ofc. Turner obtained a warrant to search the defendant’s residence (February 21, 2019) and executed that warrant (March 1, 2019). The Second Circuit has upheld warrants seeking evidence of child pornography crimes where the delay between the target’s last online activity

and the acquisition of the warrant was substantially longer than six months. *See United States v. Boles*, 914 F.3d 95, 101 (2d Cir. 2019) (calling staleness a “close question” in a case where law enforcement obtained a warrant more than 10 months after the target’s most recent online activity and ultimately upholding the warrant on the grounds of good faith); *Raymonda*, 780 F.3d 105 (finding warrant issued 9 months after the one and only date on which the target accessed thumbnail images of child pornography was stale but overturning the district court’s decision to suppress the evidence based on the good faith exception).

Ofc. Turner’s affidavit detailed three instances in which a computer connected to the Network from the defendant’s residence attempted to download child pornography. Ofc. Turner explained that the defendant had a prior conviction of possessing child pornography (Turner Aff. ¶ 71), making him less likely to be a one-, two-, or three-time downloader of child pornography and more likely to be a collector. Ofc. Turner also explained that, based on his training and experience, “those who distribute and possess child pornography often maintain their collections that are in a digital or electronic format in a safe, secure and private environment, such as a computer, or other digital device, and surrounding area . . . for several years.” (Id., ¶ 72(d).)

The defendant’s repeated download attempts and prior conviction and Ofc. Turner’s training and experience all supported Judge Payson’s conclusion that there was probable cause to believe evidence of child pornography crimes would still be present in the defendant’s residence six months after his last attempted download. Accordingly, the warrant was not stale and the defendant’s motion to suppress the evidence seized from his residence based on staleness should be denied.

c. The Defendant's Request for a Franks Hearing Should Be Denied Because Ofc. Turner Did Not Intentionally Mislead the Court

“There is ... a presumption of validity with respect to the affidavit supporting [a] search warrant,” *Franks v. Delaware*, 438 U.S. 154, 171 (1978). “To show entitlement to a hearing under *Franks*, a defendant must make a ‘substantial preliminary showing’ that (1) any inaccuracies in the affidavit supporting the warrant were made ‘knowingly and intentionally, or with reckless disregard for the truth,’ and (2) such inaccuracies were ‘necessary to the finding of probable cause.’” *United States v. Torres-Fernandez*, No. 21-19, 2021 WL 4944455, at *1 (2d Cir. Oct. 25, 2021)) (quotation omitted)).

i. The defendant has failed to demonstrate that Ofc. Turner's warrant affidavit contained any inaccuracies or omissions that were necessary to the finding of probable cause

The defendant's motion alleges Ofc. Turner's affidavit contains three inaccuracies and omissions: (a) it inaccurately describes how Freenet distributes requests among peers, (b) it omits the “percentage of even share” for each request, and (c) it omits the timing of each request.

The defendant's predominant argument is that Ofc. Turner's affidavit inaccurately described how Freenet distributes requests of blocks among peers. However, in every instance where Ofc. Turner discusses the distribution of requests, he clearly states that they are “roughly” divided among a user's peers, not exactly. (*See, e.g.*, Turner Aff., ¶¶ 15 (“the Network software divides the requests for blocks into roughly equal amounts among the requesting user's peers”), 16 (“if User ‘A’ has 10 peers and requests 1000 blocks of a file, roughly 100 blocks are requested from each one of User A's peers”), 45 (“relying on the fact

that an original requestor is divided in approximately equal parts between each of the original requestor's peers and an intermediary or second-level request is subdivided evenly between the intermediary user's peers (see Figures 1 and 2), the Formula determines whether it is more probable than not that a request received by a law enforcement computer for a specific number of blocks of a known 'file of interest' was received from an original requestor or a mere intermediary") (emphasis added).)

In his discussion of the Formula, Ofc. Turner is clear that the division is approximate, not exact, by selecting a request number that fell outside of the predicted range:

48. If User X were the original requestor, then a recipient of a request from User X would expect to receive a request for somewhere between 120 blocks (6,000 minimum necessary blocks/50 peers) and 240 blocks (12,000 maximum necessary blocks/50 peers).

49. If, in the alternative, User X were a second level requestor, then User X likely received a request from the original user for anywhere from 750 blocks (6,000 minimum required blocks/8 peers) to 1,500 blocks (12,000 maximum required blocks/8 peers). A recipient of a second-level request from User X would then expect to receive a request for anywhere from approximately 15 blocks (750 requested blocks/50 peers) to 30 blocks (1,500 blocks/50 peers).

50. Note that the number of requests the law enforcement computer receives if User X is an original requestor is substantially larger (often by a factor of 10) than the number of requests the law enforcement computer would receive if User X were merely a second level or intermediary requestor.

51. In this example, the law enforcement computer received a request for 100 blocks. That request **falls much closer to the expected range** for an original request from User X (120-240). In contrast, a request for 100 blocks is substantially greater than the expected range for a second level request from User X (15-30 blocks). Therefore, there is a high probability that User X was the original requestor of File of Interest A.

(Turner Aff., ¶¶ 48-49, 51 (emphasis added).)

Even the results generated by the application of the Formula to the download requests at issue showed that it generated an estimate because the actual number of requests fell outside of the Formula's estimated range. For the September 9, 2018 download, the Formula estimated that an original request would seek approximately 127-250 blocks; a second level request would seek approximately 15-31 blocks. The actual request was for 126 blocks. (*Id.*, ¶ 62.) Similarly, for the September 11, 2018 download, the Formula estimated that an original request would seek approximately 92-182 blocks; a second level request would seek approximately 11-23 blocks. The actual request was for 69 blocks. (*Id.*, ¶ 63.)

Ofc. Turner disclosed that the division of requests was approximate, not exact. His description of Freenet was not false. The probable cause inquiry does not require him to go further and give a hyper technical explanation of Freenet's design and operation, in theory and in practice, because a more detailed explanation would not affect the relevant inquiry—whether the Formula works in practice. Thus, even if his description of Freenet was false (which it was not), it was not materially false.

Similarly, the defendant argues Ofc. Turner's affidavit did not disclose the "percentage of even share data" for each request he received from the defendant's computer. The defendant fails to explain what this metric is or why it is relevant to the probable cause inquiry.

Finally, the defendant alleges that Ofc. Turner failed to disclose data on the timing of requests he received from the defendant's computer. That is factually incorrect because, in each instance where Ofc. Turner's affidavit discusses a request, he provides the timing of that request. (Turner Aff., ¶¶ 61 ("on August 8, 2018, between 10:07 PM and 10:44 PM UTC"), 62 ("On September 9, 2018, between 10:34 AM and 1:30 PM UTC"), and 63 (On Tuesday, September 11, 2018, between 12:32 AM and 4:09 AM UTC").)

In sum, the defendant has failed to identify a single materially false representation in Ofc. Turner's affidavit.

ii. The defendant has not made any showing that the alleged inaccuracies were made knowingly, intentionally, or recklessly

The defendant's motion leaves out the most important part of the *Franks* hearing analysis. The defendant needed to make a substantial showing that Ofc. Turner knew of (or recklessly disregarded) the alleged inaccuracies and intentionally mislead the Court.

Quite the contrary, as the affidavit lays out, all the information at Ofc. Turner's disposal—his training, his experience, his conversations with other members of law enforcement, and his review of applicable case law—told him that the Formula was a reliable method for assessing the likelihood that evidence of child pornography would be found at a particular location.⁷

First, Ofc. Turner's affidavit states he received training regarding the operation of the Network software and the use of the Formula (Turner Aff., ¶ 31) and in child pornography investigations (*id.*, ¶ 72).

Second, Ofc. Turner reasonably relied upon his training, his experience, and the experience of other law enforcement officers in this area. The fact that the defense cannot locate more than five published opinions regarding search warrant affidavits that employ the

⁷ The defendant's motion repeatedly mischaracterizes the relevant inquiry. The question is not whether there was probable cause to believe the defendant was downloading child pornography (*see, e.g.*, Def. Motion, Dkt. 62, ¶ 11). The question is whether there was probable cause to believe there was evidence of the possession or receipt of child pornography in the defendant's residence.

Formula is irrelevant. As the Court is aware, only a very small percentage of search warrant affidavits are ever discussed in a published opinion. Most search warrant affidavits are seen only by the officers, prosecutors, courts, and (where charges result) defendants involved in a particular case. They are not posted on Westlaw, Lexis, or any other searchable database.⁸

Third, Ofc. Turner reasonably relied upon the carefully considered decision in *United States v. Dickerman*, 16-CR-0258-HEA, 2017 WL 11485604 (E.D. Mo. Sept. 26, 2017). The defendant's motion discusses this decision at length but never mentions the ultimate conclusion: the Court found the Formula applied in *Dickerman* and this case supported a finding of probable cause and upheld the warrant. This holding was adopted by the District Court (16-CR-0258-HEA, 2018 WL 10228437 (E.D. Mo. Apr. 27, 2018)), and affirmed by the Eighth Circuit (954 F.3d 1060 (8th Cir. 2020)).

The defendant tries to distinguish *Dickerman* from this case by comparing the timing of the requests, "actual percentage of requests," and "false percentage of even share." (Def. Motion, Dkt. 62, p. 37-38.) He alleges these were "considered important in the *Dickerman* case." (*Id.*, p. 40.)

But the *Dickerman* affidavit—which was upheld—did not contain any of the information that the defendant alleges is missing from Ofc. Turner's affidavit. A copy of the *Dickerman* search warrant affidavit is attached hereto as Exhibit 1. It is a four-page affidavit that provides the following information about a single download request:

⁸ Case in point, in the *Dickerman* evidentiary hearing (which the defense quotes extensively) Investigator Becker testified that he had been involved in 40 or 50 Freenet investigations and, in every case, he found evidence of child pornography on the target computer. (*Dickerman* Evidentiary Hearing, Dkt. 62-5, p.9.)

6. While reviewing requests received by undercover *Freenet* nodes, located in Missouri, SI Becker observed IP address 172.12.235.62 routing and/or requesting suspected child pornography file blocks. The number and timing of the requests was significant enough to indicate that the IP address was the apparent original requester of the file.

7. SI Becker observed that on April 2, 2015 between 11:08PM UTC and 11:10PM UTC a computer running *Freenet* software, at IP address 172.12.235.62, requested from Freenet law enforcement nodes 69 parts, or blocks, of the e following file:

SHA1: *BODS262HHKS3VS4FLQSOAAVAWTOE5FAW*

File Name: *Anonther Set 2 (set 2).zip*

SI Wayne Becker has downloaded this video file with the referenced SHA1 value from *Freenet* and it is described as follows:

Description: This folder contains 17 jpg images, all off a female child, 3-5 years of age. In all of the images she is wearing only a night shirt and it is pulled up. Her legs are spread displaying her genitals. An adult males hand can be seen spreading her buttocks for the camera in 2 of the images. In 4 of the images an unseen male's penis is penetrating the child anally.

8. On August 12, 2015 this affiant viewed the above listed files and observed that they contained the imagery described above that this affiant believes to be child pornography.

Moreover, the Magistrate Judge's decision in *Dickerman* did not highlight or rely on any metric that the defendant alleges is missing from Ofc. Turner's affidavit.

Collectively, Ofc. Turner's training and experience and existing case law gave him a reasonable belief that the Formula was reliable. The defense has not pointed to a single thing that was within Ofc. Turner's knowledge that would have given him or the Court pause before relying upon the Formula to obtain a search warrant.

Because the defendant failed to make a substantial preliminary showing that there were any material inaccuracies in Ofc. Turner's affidavit and that any of those alleged inaccuracies were made knowingly, intentionally, or with reckless disregard for the truth, the defendant's motion for a *Franks* hearing should be denied. See *United States v. Popa*, 369 F.

Supp. 3d 833, 839 (N.D. Ohio 2019) (denying motion for a *Franks* hearing and motion to suppress warrant based on same Formula).

d. The Good Faith Exception to the Exclusionary Rule Applies in this Case

“Even where a warrant was issued without probable cause in violation of the Fourth Amendment, suppression of the evidence is not automatic.” *Jones*, 43 F.4th at 110 (quotation omitted). “The exclusionary rule is a judicially created doctrine that is prudential rather than constitutionally mandated. It therefore applies only where its deterrence benefits outweigh its substantial social costs. The extent to which the exclusionary rule is justified by deterrence principles varies with the culpability of the law enforcement conduct.” *Id.* (quotations omitted).

“Because the exclusionary rule exacts a heavy toll on the justice system, it applies only to deter law enforcement’s deliberate, reckless, or grossly negligent conduct.” *Id.* (quotations omitted). “In accord with these principles, the ‘good-faith exception’ to the exclusionary rule applies when the agents executing a search warrant act with an objectively reasonable good-faith belief that their conduct is lawful.” *Id.* (quotation omitted).

For the reasons discussed above, Ofc. Turner clearly acted in good faith when he applied for and relied upon the warrant in this case. Because there is no evidence of bad faith on Ofc. Turner’s part, the Court can and should forego the probable cause and *Franks* analysis and deny the defendant’s motion on this ground alone. *See United States v. Dickerman*, 954 F.3d 1060, 1069 (8th Cir. 2020) (affirming a district court’s denial of a motion to suppress regarding a warrant that employed the Formula based on the *Leon* good-faith exception and therefore declining to reach the underlying question of probable cause).

B. THE DEFENDANT’S MOTION FOR A BILL OF PARTICULARS SHOULD BE DENIED

“The fundamental question a court must answer when deciding whether to order particularization is whether the information sought is necessary, not whether it is helpful.” *United States v. Nagi*, 254 F. Supp. 3d 548, 562 (W.D.N.Y. 2017) (quotation omitted). “[A] bill of particulars is not a discovery device, nor is it a way for a defendant to obtain a preview of the manner in which the Government will attempt to prove the charges, or the means by which the crimes charged were committed.” *Id.* at 563 (quotation omitted). Accordingly, “[a] bill of particulars should therefore be ordered only where the charges of the indictment are so general that they do not advise the defendant of the specific acts of which he is accused,” and would subject the defendant to “unfair surprise at trial if he did not receive particularization.” *Id.* at 562 (quotations omitted).

In this case, the indictment charges that on or about March 1, 2019, the defendant possessed child pornography on three specific devices: a Hewlett Packard Pavilion dvG Laptop Computer; Model: dvGt-7000; S/N: 2CE31510XV (Count 1); a Hewlett Packard Pavilion dv7 Laptop Computer; Model: dv7t-6c00; S/N: 2CE2011X6Y (Count 2); and a Hewlett Packard Pavilion dvG Laptop Computer; Model: dv6t-6c00; S/N: 2CE2052K0H (Count 3). The government has made the full contents of those devices available to the defense. They contain all the images of child pornography that the government alleges the defendant possessed.

The Indictment alleges a specific and narrow date range for the defendant’s conduct and the precise materials the defendant used to commit the charged offenses. And the government has made all of the images available in discovery. There is no risk that the

defendant will face future charges related to his possession of the three HP laptops, in violation of the Double Jeopardy Clause. And, because the government has made all of the images available, there is no risk that the defendant will be surprised at trial by an image that he and his counsel have never had an opportunity to review. Thus, the defendant has no need for a bill of particulars.

The law does not require the government to specify the exact images at issue in either the Indictment or a bill of particulars. *United States v. Anson*, 304 F. App'x 1 (2d Cir. 2008) (rejecting a defendant's challenge to the specificity of an indictment charging him with receipt and possession of child pornography and holding that the indictment did not need to describe in detail the images that correspond to each count); *United States v. Brose*, No. 10-CR-265S, 2011 WL 6140545, at *3 (W.D.N.Y. Dec. 9, 2011) ("the indictment here clearly describes the material at issue—an IBM 10 GB hard drive bearing serial number 42V42GY8845—and thus provides Defendant with sufficient notice of the charges and with enough detail to plead double jeopardy in future prosecutions for the same events"); *United States v. White*, No. 07-CR-1345, 2008 WL 5234340 (W.D.N.Y. Dec. 12, 2008) (denying defendant's request for bill of particulars specifying the particular images of child pornography the defendant was accused of possessing on a CD and noting the government had made the full contents of the CD available to the defense for inspection).

The defendant's argument that "one juror may think [the defendant] possessed one image of child pornography, and another juror may disagree, but believe [the defendant] accessed another image with the same intent" (Def. Motion, Dkt. 62, p. 58-59) is not grounds for a bill of particulars. Rather, the issue of unanimity is routinely and more appropriately

through a jury instruction. See, e.g., *United States v. Anson*, No. 04-CR-6180 CJS, 2007 WL 119150, at *3 (W.D.N.Y. Jan. 10, 2007), *aff'd*, 304 F. App'x 1 (2d Cir. 2008) (quoting unanimity instruction given to jury during child pornography trial).

The defendant's argument that "the government need specify on which particular device these image(s) were received" (Def. Motion, Dkt. 62, p. 59) is nonsensical. The Indictment does specify the three devices that the government alleged contained child pornography.

As is set forth above, the Indictment tracks the elements of the charged offenses, alleges the defendant committed the charged offenses within a narrow date range, and alleges the specific material used to commit the offenses. In addition, the government has provided ample discovery. As such, the defendant does not need further particularization of his charges and his request for a bill of particulars should be denied.

C. DISCOVERY, *BRADY*, *JENKS*, CHARACTER EVIDENCE, AND RAW NOTES

The government will promptly produce to the defendant any additional Rule 16 materials that come into its possession.

The government acknowledges its obligation to advise the defense promptly of any known information that is favorable and material to the defense. See *Brady v. Maryland*, 373 U.S. 83, 87 (1963). Impeachment material (*Giglio* material), to the extent it exists, will be disclosed sufficiently in advance of trial to permit the defense time to prepare for cross-examination.

The government will timely produce witness statements in accordance with the requirements of the Jencks Act, 18 U.S.C. § 3500. The government is cognizant of the goal of avoiding interruptions at trial and will produce witness statements sufficiently in advance to avoid such interruptions.

The government has instructed its agents to preserve all rough notes in existence as of the date of this response.

The government will comply with the requirements of the Rules of Evidence, including Rules 404(b), 608 and 609. The government respectfully suggests that questions about the timing regarding any required notice and admissibility of any evidence will be addressed by the trial judge.

D. RECIPROCAL DISCOVERY

Pursuant to Rule 16(b) of the Federal Rules of Criminal Procedure, the government requests that defendant timely provide to the government the materials and information set forth in Rule 16(b)(1), including documents and objects, reports of examinations and tests, and expert witnesses.

E. DEMAND FOR NOTICE OF ALIBI

Pursuant to Rule 12.1 of the Federal Rules of Criminal Procedure, the government requests that the defendant notify the government of any intended alibi defense within 14 days or at some other time designated by the Court.

Dated: Rochester, New York
October 19, 2022

TRINI E. ROSS
United States Attorney

By: s/Meghan K. McGuire
MEGHAN K. MCGUIRE
Assistant United States Attorney
U.S. Attorney's Office
100 State Street, Suite 500
Rochester, NY 14614
(585) 399-3922
Meghan.McGuire@usdoj.gov